(19) Japan Patent Office (JP)

(12) Publication of Patent Application (A)

(11) Publication of Patent Application No. H10-271154

(43) Date of Publication of Application: October 9, 1998

---

(51) Int Cl.[6]	Identification Number	FI	
H04L	12/46	H04L 11/00	310C
	12/28	9/00	671
	9/32		685
	9/36	11/20	102Z
	12/58		

Request for Examination: not made

Number of Claims: 10 (10 pages in total)

---

(21) Application Number: Japanese Patent Application No. H9-67929

(22) Application Date: March 21, 1997

(71) Applicant: 000232047
NEC Engineering Co., Ltd.
18-21, Shibaura 3-chome, Minato-ku, Tokyo

(72) Inventor: Yoshie Matsuoka
c/o NEC Engineering Co., Ltd.
18-21, Shibaura 3-chome, Minato-ku, Tokyo

(74) Agent: Patent Attorney, Seigou Suzuki

---

(54) Title of the Invention:

ILLEGAL ACCESS PREVENTION METHOD AND SYSTEM

(57) [Abstract]

[Problem to be Solved]

To allow elimination of a bad packet by filtering using an existing area of the packet without adding an area to the data format of the packet.

[Solution]

An IP header check unit 11 of a gateway 1 allows only a good communication packet to pass through, based on TTL (Time To Live) information and IP address information that are included in the IP header. A TTL filtering unit 21 of the IP header check unit 11 allows only a communication packet with valid TTL information in the IP header, to pass through. A validity check unit 21a checks validity based on the condition that the value of the TTL of a passing packet is within the range of the initial value determined in advance in a group, to a value (the initial value minus the maximum number of passing gateways). A filtering processor 21b gives a communication packet with TTL information not satisfying the given condition, to a packet discard unit 12.

[Claims for the Patent]

[Claim 1]

An illegal access prevention method used in a communication network including a plurality of branch networks connected by connecting devices, in which one or more logical groups are formed, to prevent illegal access in the logical group,

wherein the method is characterized in that the initial value of the Time To Live information included in a communication packet, is set in advance at the time of the transmission, to a predetermined value as confidential information in the logical group,

wherein the connecting device checks the validity of the Time To Live information when the communication packet passes therethrough, for the purpose of filtering of the packet passing in and out of the logical group.

[Claim 2]

The illegal access prevention method according to claim 1, characterized in that the Time To Live information includes information to be subtracted each time the packet passed through each of the connecting devices,

wherein the initial value of the Time To Live information as confidential information, is set to a value exceeding the estimated maximum number of connecting devices through which the packet is supposed to pass, based on the network configuration,

wherein, when the value of the Time To Live information of the passing packet is out of the range of

the initial value to the value (the initial value minus the maximum number of connecting devices through which the packet is supposed to pass), the connecting device determines that the packet is a bad packet.

[Claim 3]

The illegal access prevention method according to claim 1 or 2, characterized by further using filtering based on IP (Internet Protocol) address.

[Claim 4]

The illegal access prevention method according to any one of claims 1 to 3, characterized by further using filtering based on MAC (Media Access Control) address.

[Claim 5]

The illegal access prevention method according to any one of claims 1 to 4, characterized in that the bad packet is discarded by the connecting device.

[Claim 6]

An illegal access prevention system used in a communication network including a plurality of branch networks connected to each other, in which one or more logical groups are formed,

wherein the system is characterized by comprising:

a terminal device connected to the branch network, having Time To Live information setting means for setting the initial value of the Time To Live information included in a communication packet at the time of the transmission of the communication packet, to a predetermined value as confidential information in the logical group set in

advance in the communication network; and

network connecting means having validity check means for checking the validity of the Time To Live information of the communication packet passing therethrough, and filtering processing means for filtering the packet passing in and out of the logical group based on the check result of the validity check means,

wherein the network connecting means connects the plurality of branch networks while preventing illegal access in the logical group.

[Claim 7]

The illegal access prevention system according to claim 6, characterized in that the Time To Live information includes information to be subtracted each time the packet passed through each of the network connecting means,

wherein the Time To Live information setting means includes means for setting the initial value of Time To Live information as confidential information, to a value exceeding the estimated maximum number of network connecting means through which the packet is supposed to pass, based on the network configuration,

wherein the validity check means includes means for determining that the packet is a bad packet, when the value of the Time To Live information is out of the range of the initial value to the value (the initial value minus the maximum number of network connecting means through which the packet is supposed to pass).

[Claim 8]

The illegal access prevention system according to claim 6 or 7, characterized in that the network connecting means further includes IP address filtering means for performing filtering based on IP (Internet Protocol) address.

[Claim 9]

The illegal access prevention system according to any one of claims 6 to 8, characterized in that the network connecting means further includes MAC address filtering means for performing filtering based on MAC (Media Access Control) address.

[Claim 10]

The illegal access prevention system according to any one of claims 6 to 9, characterized in that the network connecting means includes packet discard means for discarding the bad packet prevented from passing through by filtering.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to preventing illegal access in routers, gateways, or other devices that form a communication network system. More particularly, the present invention relates to an illegal access prevention system suitable for communication network systems using TCP/IP (Transmission Control Protocol/Internet Protocol) as a communication protocol.

[0002]

[Prior Art]

A communication network system, for example, a LAN (Local Area Network) system, is formed by connecting a plurality of branch LANs through at least either routers or gateways. In such a communication network system, TCP/IP is often used as a communication protocol.

[0003]

Some networks are physically connected, on which logical grouping is done according to necessity. In such a case, communication takes place mostly within a logical group, and communication with other groups may not be necessary or is desired to be eliminated.

[0004]

In such a case, in the routers, gateways, or other devices that connect the branch LANs, the MAC (Media Access Control) addresses or IP (Internet Protocol) addresses of packets are identified to prevent a packet of another group from passing through, in order to prevent an illegal access packet such as a multicast packet, an abnormal packet, or a packet trying to illegally access a terminal of another group, from entering into and going out of the specific group.

[0005]

As described above, the function of identifying the MAC addresses or IP addresses of packets to prevent a packet of another group from passing through, is called MAC address filtering function for performing filtering based

on MAC address, or called IP address filtering function for performing filtering based on IP address.

[0006]

In other words, the filtering based on MAC address or IP address is performed in the following manner. The MAC address or IP address that allows a packet to pass through, is registered in advance in the router or gateway. The router or gateway checks the MAC address or IP address of the received packet against the registered MAC address or IP address, allowing only the packet with the correct MAC address or IP address to pass through. In this way, the passing of the illegal access packet is prevented by the router or gateway.

[0007]

In many cases, the MAC address is physically set to a terminal device (hereinafter simply referred to as "device") and is unlikely to be easily changed. However, there exists a multicast address in the MAC layer address to allow a multicast packet to pass through all networks, causing confusion with the multicast packet. In order to prevent such confusion, IP address filtering is used for filtering based on IP address in the network layer above the MAC layer.

[0008]

However, the IP address, which is necessary for the TCP/IP protocol, is logically set to the device and can be relatively easily changed. For this reason, when a device not belonging to a specific group, illegally sets the IP

address of a terminal of the group to try to enter the LAN system in the same group, the illegal access packet may not be reliably detected by IP address filtering.

[0009]

To overcome the above problem, Japanese Patent Application Laid-Open No. H7(1995)-170279 discloses a technology for eliminating an illegal address packet without using IP address filtering.

[0010]

In other words, the system disclosed in JP-A No. H7(1995)-170279 uses, in addition to the conventional bridge circuit that accommodates a plurality of branch LANs and performs filtering based on MAC address, a bridge circuit having a function for registering the group number of each branch LAN, a function for adding the group number to a packet at the time of the transmission, and a function for checking the group number added to the packet against the registered group number at the time of receiving the packet.

[0011]

That is, the system sets the group number to each of the LANs accommodated in each of the bridge circuits, and adds the group number to a packet to be transmitted to a core bus to transfer data between LANs in the same group. When the packet is received from the core bus, the system performs filtering based on the group number added to the packet at the time of the transmission, before performing filtering based on MAC address, which is the filtering

function the bridge circuit originally performed.

[0012]

In other words, in the system formed by connecting a plurality of branch LANs to which a plurality of terminals are connected, to a core bus through a plurality of bridge circuits, the plurality of LANs, which are respectively accommodated in the plurality of bridge circuits, are grouped into a plurality of independent groups. The group number of each branch LAN is registered in advance in each bridge circuit in which the branch LAN is accommodated. When a packet is transmitted from a terminal to another branch LAN in the same group, the bridge circuit adds to the packet the group number of the branch LAN to which the terminal belongs, and transmits the packet along with the group number to the core bus. Upon receiving the packet through the core bus, the bridge circuit identifies the group number added to the received packet, and checks the received group number against the registered group number. Only when the two group numbers are identical, the bridge circuit applies the MAC address filtering function to the received packet, and transmits the packet to the branch LAN accommodated in the bridge circuit.

[0013]

In this way, it is possible to prevent an illegal access packet, such as a multicast packet in the MAC layer of LAN, an abnormal packet, or a packet illegally accessing a terminal of another group to communicate with a terminal of another group, by checking the difference of the group

numbers.

[0014]

[Problems to be Solved by the Invention]

As described above, the system disclosed in JP-A No. H7(1995)-170279 sets the group number for each of the plurality of branch LANs accommodated in each of the bridge circuits, and adds the group number to a packet to be transmitted to a core bus to transfer data between LANs in the same group. Upon receiving the packet from the core bus, the system performs filtering based on the group number added to the packet at the time of the transmission, before performing filtering based on MAC address which is the filtering function the bridge circuit originally performed.

[0015]

With the system of JP-A No. H7(1995)-170279, it is possible to prevent an illegal access packet such as a multicast packet in the MAC layer of LAN, an abnormal packet, or a packet illegally accessing a terminal of another group to communicate with a terminal of another group, by checking the difference of the group numbers.

[0016]

However, it is necessary to add a group number area to the packet data format, in order to enable filtering disclosed in JP-A No. H7(1995)-170279 to be performed by registering the group number to each bridge circuit, adding the group number to a packet at the time of the transmission, and upon receiving the packet, checking the

group number of the received packet against the registered group number.

[0017]

However, in many cases the LAN packet includes a header part in the physical layer, a header part in the transport layer, and the like, in which the data format of a packet is precisely defined. Thus, in the LAN system in which the packet data format is defined, it is often difficult to add and keep an area to store the group number in the existing packet, preventing the technology disclosed in JP-A No. H7(1995)-170279 from being performed.

[0018]

The present invention is made in light of the above described circumstances, and has an object to provide an illegal access prevention method and system that allow filtering of a bad packet by using an existing area of the packet, in order to effectively eliminate the bad packet without adding an area to the data format of the packet.

[0019]

[Means for Solving the Problems]

In order to achieve the above object, according to a first aspect of the present invention, there is provided an illegal access prevention method used in a communication network including a plurality of branch networks connected by connecting devices, in which one or more logical groups are formed, to prevent illegal access in the logical group. The illegal access prevention method sets in advance the initial value of the Time To Live information included in a

communication packet at the time of the transmission, to a predetermined value as confidential information in the logical group. The connecting device checks the validity of the Time To Live information when the communication packet passes therethrough, for the purpose of filtering of the packet passing in and out of the logical group.

[0020]

The Time To Live information may include information to be subtracted each time the communication packet passes through each of the connecting devices. The initial value of the Time To Live information as confidential information may be set to a value exceeding the estimated maximum number of connecting devices through which the packet is supposed to pass, based on the network configuration. When the value of the Time To Live information is out of the range of the initial value to the value (the initial value minus the maximum number through which the packet is supposed to pass), the connecting device may determine that the packet is a bad packet.

[0021]

The illegal access prevention method may further use filtering based on IP address.

[0022]

The illegal access prevention method may further use filtering based on MAC address.

[0023]

The illegal access prevention method may discard the bad packet by the connecting device.

[0024]

According to a second aspect of the present invention, there is provided an illegal access prevention system used in a communication network system including a plurality of branch networks connected to each other, in which one or more logical group are formed. The illegal access prevention system includes: a terminal device connected to the branch network, having Time To Live information setting means for setting the initial value of the Time To Live information included in a communication packet at the time of the transmission, to a predetermined value as confidential information in the logical group set in advance in the communication network; and network connecting means having validity check means for checking the validity of the Time To Live information when the communication packet passes therethrough, and filtering processing means for filtering the packet passing in and out of the logical group based on the check result of the validity check means. The network connecting means connects the plurality of branch networks while preventing illegal access in the logical group.

[0025]

The Time To Live information may include information to be subtracted each time the communication packet passes through each of the network connecting means. The Time To Live information setting means may include means for setting the initial value of the Time To Live information as confidential information, to a value exceeding the

estimated maximum number of network connecting means through which the packet is supposed to pass, based on the network configuration. The validity check means may include means for determining that the packet is a bad packet when the Time To Live information is out of the range of the initial value to the value (the initial value minus the maximum number of network connecting means through which the packet is supposed to pass).

[0026]

The network connecting means may further include IP address filtering means for performing filtering based on IP address.

[0027]

The network connecting means may further include MAC address filtering means for performing filtering based on MAC address.

[0028]

The network connecting means may include packet discard means for discarding the bad packet prevented from passing through by filtering.

[0029]

According to the present invention, the illegal access prevention method and system are used in a communication network including a plurality of branch networks connected by connecting devices, in which one or more logical groups are formed, to prevent illegal access in the logical group. The illegal access prevention method and system set the initial value of the Time to Live

information included in a communication packet at the time of the transmission, to a predetermined value as confidential information in the logical group set in advance in the communication network. The connecting device checks the validity of the Time To Live information of the communication packet passing therethrough, for the purpose of filtering of the packet passing in and out of the logical group. This allows filtering of the bad packet based on the Time To Live information which is an existing area of the packet, enabling effective elimination of the bad packet without adding an area to the data format of the packet.

[0030]

[Embodiment of the Invention]

Hereinafter, an embodiment of the present invention will be described with reference to the accompanying drawings.

[0031]

An illegal access prevention system according to an embodiment of the present invention is suitable for communication network systems using the TCP/IP protocol. In this embodiment, TTL which is an existing area in the IP header of the TCP/IP protocol, is used in filtering of a bad packet in order to effectively prevent illegal access of a communication packet with the existing data format of the communication packet kept unchanged.

[0032]

The IP header of a communication packet based on the

TCP/IP protocol includes a TTL area for storing TTL (Time To Live) information. TTL information indicates the time for which the communication packet can live in the network, namely, Time To Live, in the unit of second. With respect to the Time To Live measured by the unit of second, there may happen that the process time is less than one second or the process time is not measureable. In general, for example, each time a packet passes through each connecting device such as router or gateway, the value of the TTL information is subtracted by "1". When a communication packet with the TTL value "0" is detected, the communication packet is discarded as its Time To Live is determined to have expired. Such TTL information is provided in order to prevent occurrence of a packet being permanently undelivered and flowing in the network. In the TCP/IP protocol, the maximum value of TTL is "255 (seconds)". In general, the number of routers, gateways, or other devices from a transmitting terminal to a receiving terminal, is estimated to be larger than the true value, for the purpose of preventing occurrence of the undelivered packet. In addition, the TTL value is generally set to quite a large value, because the communication packet is discarded at a time when 255 seconds has elapsed, even if the value of the TTL has been set to the maximum value.

[0033]

In the present invention, the initial value of the TTL of a communication packet is determined in advance as

confidential information in a logical group. The maximum number of connecting devices, such as routers and gateways through which the packet is supposed to pass through from the transmitting terminal to the receiving terminal in the group, is also set in advance. The initial value of the TTL should be set to a value larger than the maximum number of connecting devices. In filtering of the packet, when the TTL value of the passing packet is in the range of the initial value of the TTL to the value (the initial value minus the maximum number of connecting devices through which the packet is supposed to pass), the packet is determined to be a normal packet. On the other hand, when the TTL value is out of the range, the packet is determined to be a bad packet.

[0034]

With such a configuration, it is possible to eliminate a bad packet transmitted from a bad terminal not belonging to a specific group to illegally access a terminal in the group by using the IP address of a terminal in the same group.

[0035]

Referring to Figs. 1 to 3, a description will be given of an embodiment of a network system including the illegal access prevention system according to the present invention based on the above described principle.

[0036]

Fig. 1 shows the configuration of the principal part of a gateway incorporating an illegal access prevention

system according to the present invention.

[0037]

In Fig. 1, a gateway 1 includes an IP header check unit 11 and a packet discard processor 12.

[0038]

The IP header check unit 11 checks IP header information, and checks packets passing from inside to outside, and from outside to inside, of the relevant group, allowing only a good communication packet to pass through while preventing a bad packet from passing. The packet discard processor 12 discards the bad packet prevented from passing through by the IP header check unit 11.

[0039]

The IP header check unit 11 includes a TTL filtering unit 21 and an IP address filtering unit 22.

[0040]

The TTL filtering unit 21 includes a validity check unit 21a and a filtering processor 21b. The TTL filtering unit 21 checks the validity of the TTL information in the IP header, allowing only the communication packet with valid TTL information as the TTL information, to pass through, while preventing the communication packet with invalid TTL information from passing.

[0041]

The validity check unit 21a checks the validity of the TTL information based on whether the TTL information in the IP header of the passing communication packet satisfies the given conditions. Of the communication packets passing

in and out of the logical group, the filtering processor 21b allows only the communication packet with the TTL information satisfying the given conditions, to pass through, on the basis of the check result of the validity check unit 21a, while giving the communication packet with the TTL information not satisfying the given conditions, to the packet discard processor 12.

[0042]

As described above, in filtering based on TTL information in the gateway 1, the initial value of the TTL in each of the logical groups is determined in advance as confidential data. Further, the maximum number of connecting devices, for example, such as gateways and routers through which a packet is supposed to pass from the transmitting terminal to the receiving terminal, is also set in advance in each of the logical groups. Then, the initial value of the TTL and the maximum number of connecting devices through which the packet is supposed to pass, are registered in advance to the validity check unit 21a of the gateway 1. In this way, the validity check unit 21a checks validity based on whether the TTL value of the passing packet is in the range of the initial value of the TTL to the value (the initial value minus the maximum number of gateways through which the packet is supposed to pass). When the TTL value is in this range, the packet is determined to be a normal packet, or valid. On the other hand, when the TTL value is out of this range, the packet is determined to be a bad packet, or invalid.

[0043]

The IP address filtering unit 22 allows communication packets from the outside of the logical group to the inside thereof, as well as communication packets from the inside of the logical group to the outside thereof, to pass through based on the IP address information in the IP headers of the packets. The IP address filtering unit 22 prevents communication packets with other IP address information from passing, and gives the communication packets to the packet discard processor 12.

[0044]

Fig. 2 shows a network system configured by using the gateway 1 shown in Fig. 1. In Fig. 2, an illegal access prevention system is configured by using a gateway having the existing filtering function, and a gateway having the filtering function according to the present invention shown in Fig. 1.

[0045]

The network system shown in Fig. 2 includes a first gateway 1, a second gateway 2, a first terminal 3, a second terminal 4, a third terminal 5, a first branch LAN 6, a second branch LAN 7, and a third branch LAN 8. The first terminal 3 and the second terminal 4 are connected to the first branch LAN 6, and the third terminal 5 is connected to the third branch LAN 8. The first branch LAN 6 and the second branch LAN 7 are connected by the second gateway 2, and the second branch LAN 7 and the third branch LAN 8 are connected by the second gateway 1.

[0046]

The first and second gateways 1 and 2 transfer data, such as communication packets, between the second branch LAN 7 and the third branch LAN 8 and between the first branch LAN 6 and the second branch LAN 7, respectively.

[0047]

The first gateway 1 is a gateway having a communication packet filtering function based on the present invention shown in Fig. 1. In other words, the first gateway 1 has the communication packet filtering function based on TTL information according to the present invention, as well as the existing communication packet filtering function based on IP address.

[0048]

The second gateway is the existing gateway, having only the communication packet filtering function based on IP address.

[0049]

It is assumed that the second terminal 4 and the third terminal 5 are members of the same group, and that the first terminal 3 does not belong to this group.

[0050]

In this case, for example, in the group of the terminals 4 and 5, it is assumed that the initial value of the TTL is set to "5" as confidential data. Further, the maximum number of connecting devices, namely, gateways through which a packet is supposed to pass, is "2" with gateways 1 and 2. These values are set in advance to the

validity check unit 21a of the gateway 1.

[0051]

The terminal 3 not belonging to the group does not know the initial value of the TTL determined between the terminals 4 and 5 in the group. Thus, it is assumed that the initial value of the TTL is set to "32" in the terminal 3. Referring to the flowchart shown in Fig. 3, a description will be given of the operation of the terminal 4 transmitting a communication packet to the terminal 5, as well as the operation of the terminal 3 trying to illegally access the terminal 5 with the IP address of the terminal 4 by pretending to be the terminal 4 not connected to the branch LAN 6. The flowchart of Fig. 3 shows a flow of IP header check process in the IP header check unit 11 of the gateway 1 shown in Fig. 1.

[0052]

The gateway 2 only filters IP addresses, so that IP addresses of the terminals 4 and 5 are registered in the gateway 2. While in the gateway 1, the IP addresses of the terminals 4 and 5 are registered to filter IP addresses. At the same time, the TTL initial value α "5" determined between the terminals 4 and 5, as well as "2" which is the maximum number of gateways through which a packet is supposed to pass, are stored in the validity check unit 21a of the gateway 1.

[0053]

First, a description will be given of the operation of the terminal 4 transmitting a communication packet to

the terminal 5 belonging to the same group.

[0054]

The terminal 4 sets the own IP address, the source IP address, to the IP address of the terminal 4, and sets the other side's IP address, the (transmission) destination IP address, to the IP address of the other side's terminal 5. The terminal 4 also sets the TTL to the initial value α "5" that is determined between the terminals 4 and 5 in the group, and transmits the communication packet to the branch LAN 6.

[0055]

The transmitted packet is received by the gateway 2. The gateway 2 checks the IP header of the received packet. In this case, the source IP address is the registered address of the terminal 4, and the destination IP address is the registered address of the terminal 5. Thus, the gateway 2 determines that the packet is a normal packet. When determining the packet to be normal, the gateway 2 sets the TTL to "4" as a new TTL value, which is obtained by subtracting "1" from the original TTL value "5". Then, the gateway 2 transmits the communication packet to the branch LAN 7.

[0056]

The packet transmitted to the branch LAN 7 is further received by the gateway 1. The gateway 1 checks the IP header of the received packet by the IP check unit 11 according to the flowchart shown in Fig. 3.

[0057]

When IP header check is started, the version of the IP is checked (step S11). When the version is detected to be abnormal, the packet is discarded by the packet discard processor 12 (step S17). When the version is detected to be normal in step S11, other information of the IP header is checked (step S12). When the other information is detected to be abnormal, the process moves to step S17 to discard the packet.

[0058]

When the other information is detected to be normal in step 12, the TTL value is checked to determine whether the value is "0" or not (step S13). When the TTL value is "0" in step S13, the TTL, namely, Time To Live has expired, and the packet is discarded in step S17. In this case, the TTL value is "4", so that the packet is determined to be normal in step S13. Then, the validity of the TTL value is checked by the validity check unit 21a of the TTL filtering unit 21 (step S14).

[0059]

The validity check is performed based on whether the TTL value is equal to or less than the initial value α and exceeding the value β (the initial value minus the maximum number of gates). When the TTL value is in this range, it is determined to be valid.

[0060]

In this case, the initial value α is "5", the value β (initial value minus the maximum number of gates) is "3" (=5-2), and the TTL value of the received packet is "4".

Thus, the received packet is determined to be normal. When the packet is determined to be normal in step S14, the IP address of the packet is checked by the IP address filtering unit 12 (step S15). When the packet is determined to be bad in step S14, the packet is discarded in step S17.

[0061]

Because the source IP address of the received communication packet is the registered IP address of the terminal 4, as well as the destination IP address is the registered address of the terminal 5, the communication packet is determined to be a normal packet and is received by the gateway 1 (step S16). The gateway 1 sets the TTL of the received packet to "3" obtained by subtracting "1" from "4", and transmits the communication packet to the branch LAN 8. The transmitted communication packet is received by the terminal 5 which is the destination terminal.

[0062]

Next, a description will be given of the operation of the terminal 3, which is not belonging to the relevant group, trying to illegally transmit a packet to the terminal 5 by pretending to be the terminal 4 not connected to the branch LAN 6.

[0063]

The terminal 3 sets the source IP address to the IP address of the terminal 4, and sets the destination IP address to the IP address of the destination terminal 5. Then the terminal 3 transmits the communication packet to

the branch LAN 6. However, in this case, because the terminal 3 does not belong to the logical group to which the destination terminal 5 belongs, the terminal 3 does not know the TTL initial value determined in the relevant group. For this reason, the terminal 3 sets the TTL to an arbitrary value of "32", and transmits the communication packet.

[0064]

The transmitted communication packet is received by the gateway 2. The gateway 2 checks the IP header of the received packet to filter the IP address. In this case, as the source IP address is the registered address of the terminal 4, and the destination IP address is the registered address of the terminal 5, the gateway 2 determines that the IP address is normal. Thus, the gateway 2 sets the TTL to "31" obtained by subtracting "1" from "32", and transmits the communication packet to the branch LAN 7.

[0065]

The packet transmitted to the branch LAN 7 is received by the gateway 1. The gateway 1 checks the IP header of the received packet by the IP header check unit 11 according to the flowchart shown in Fig. 3.

[0066]

When IP header check is started, the version of the IP is checked in step S11. When the version is detected to be abnormal, the process moves to step S17 and the packet is discarded by the packet discard processor 12. When the

version is normal in step S11, other information of the IP header is checked in step S12. When the other information of the IP header is detected to be abnormal, the packet is discarded in step S17.

[0067]

When the other information of the IP header is normal in step S12, the TTL value is checked to determine whether the value is "0" or not in step S13. The packet will be discarded if the TTL value is "0" in step S13. However, in this case, the TTL value is "31", so that it is determined to be normal in step S13. Then, the validity of the TTL value is checked in step S14.

[0068]

In the validity check in step S14, as described above, the initial value α is "5" and the value β (the initial value minus the maximum number of gateways through which the packet is supposed to pass) is "3" (=5−2), but the TTL value of the received communication packet is "31". Thus, the packet is determined to be abnormal, and the process moves to step S17 to discard the communication packet.

[0069]

As described above, with the filtering function based on the TTL in the IP header, it is possible to detect a bad packet, which is undetectable by IP address filtering, and discard the bad packet to increase the reliability in the illegal access prevention function of the terminal.

[0070]

Incidentally, in the embodiment of the present

invention described with reference to Figs. 1 to 3, filtering based on TTL information is used in combination with filtering based on IP address. However, it is also possible to combine with a MAC address filtering function by further providing means for performing filtering based on MAC address.

[0071]

[Advantages of the Invention]

As described above, the illegal access prevention method and system according to the present invention, are used in a communication network including a plurality of branch networks connected by connecting devices, in which one or more logical groups are formed, to provide illegal access in the logical group. The illegal access prevention method and system set the initial value of the Time To Live information included in a communication packet at the time of the transmission, to a predetermined value as confidential information in the logical group set in advance in the communication network. The connecting device checks the validity of the Time To Live information of the communication packet passing therethrough, for the purpose of filtering of the packet passing in and out of the logical group. This allows filtering of the bad packet based on the Time To Live information which is an existing area of the packet.

[0072]

In other words, according to the present invention, it is possible to provide the illegal access prevention

method and system that allow filtering of a bad packet based on an existing area of the packet, in order to effectively eliminate the bad packet without adding an area to the format of the packet.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a block diagram showing the configuration of the principal part of a gateway incorporating an illegal access prevention system according to an embodiment of the present invention.

[Fig. 2] Fig. 2 is a block diagram showing the configuration of a network system using the gateway of Fig. 1.

[Fig. 3] Fig. 3 is a flowchart showing the flow of IP header check in an IP header check unit of the gateway, which explains the operation of the system of Fig. 1.

[Description of Symbols]

1, 2: gateway

3 to 5: terminal (terminal device)

6 to 8: branch LAN (Local Area Network)

11: IP (Internet Protocol) header check unit

12: packet discard processor

21: TTL (Time To Live) filtering unit

21a: validity check unit

21b: filtering processor

22: IP address filtering unit

FIG. 1

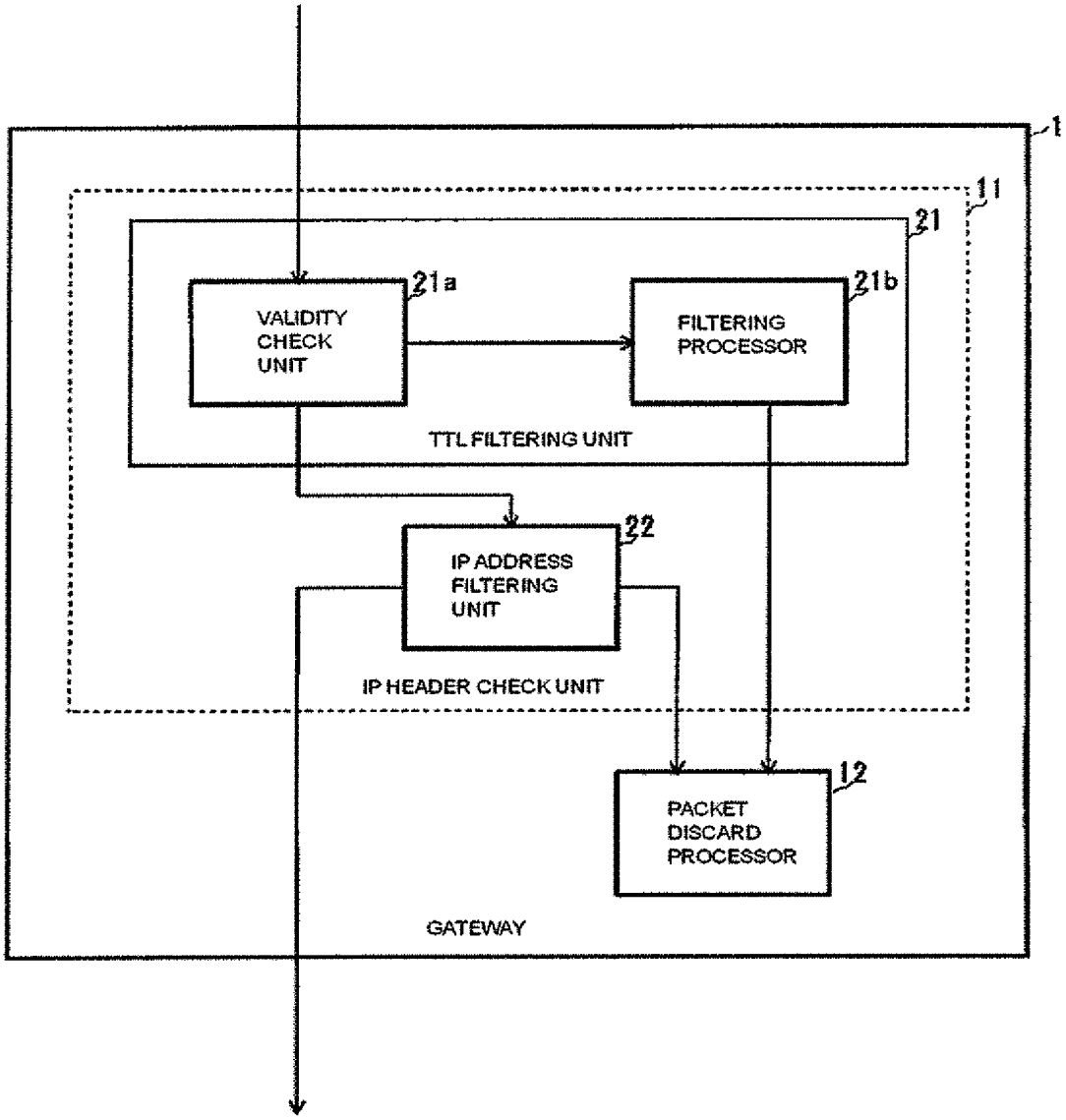

1
11
21
21a
VALIDITY CHECK UNIT
21b
FILTERING PROCESSOR
TTL FILTERING UNIT
22
IP ADDRESS FILTERING UNIT
IP HEADER CHECK UNIT
12
PACKET DISCARD PROCESSOR
GATEWAY

FIG. 2

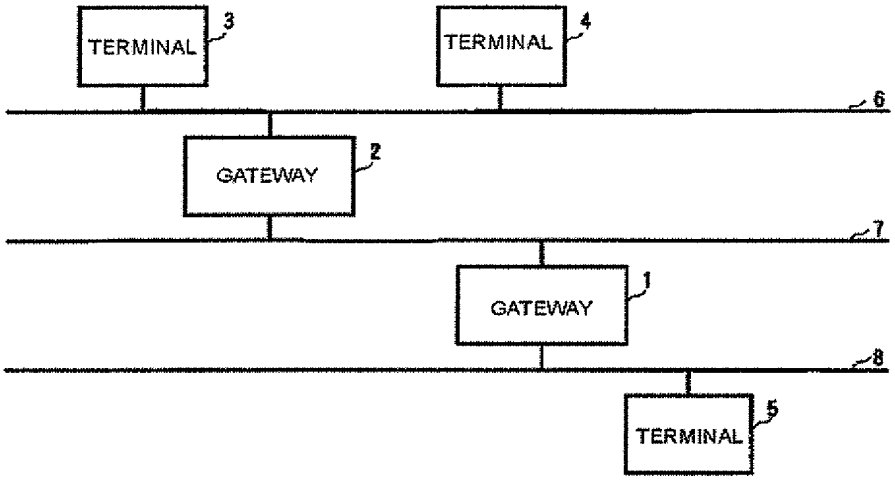
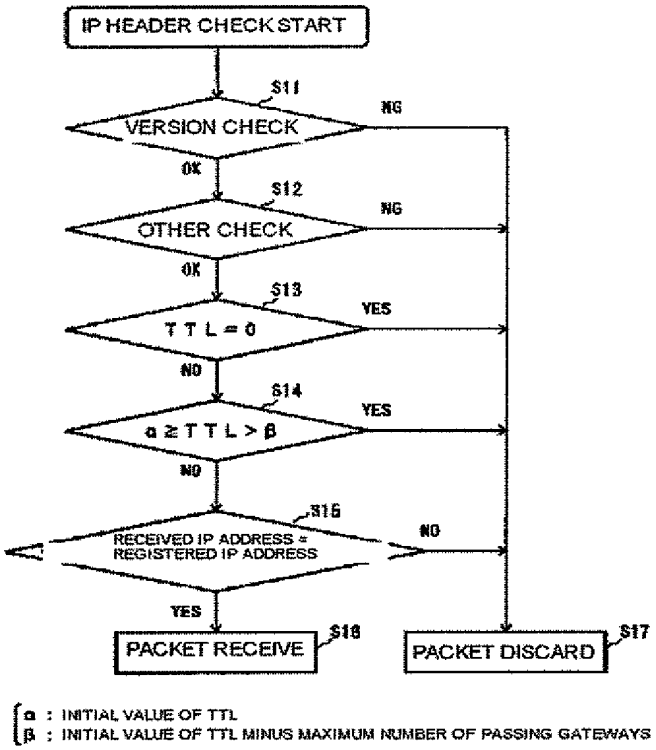


FIG. 3


IP HEADER CHECK START
S11
VERSION CHECK
NG
OK
S12
OTHER CHECK
NG
OK
S13
TTL = 0
YES
NO
S14
α ≥ TTL > β
YES
NO
S16
RECEIVED IP ADDRESS = REGISTERED IP ADDRESS
NO
YES
PACKET RECEIVE
S18
PACKET DISCARD
S17
α : INITIAL VALUE OF TTL
β : INITIAL VALUE OF TTL MINUS MAXIMUM NUMBER OF PASSING GATEWAYS

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－271154

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　11/00	３１０Ｃ
12/28		9/00	６７１
9/32			６８５
9/36		11/20	１０２Ｚ
12/56			

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

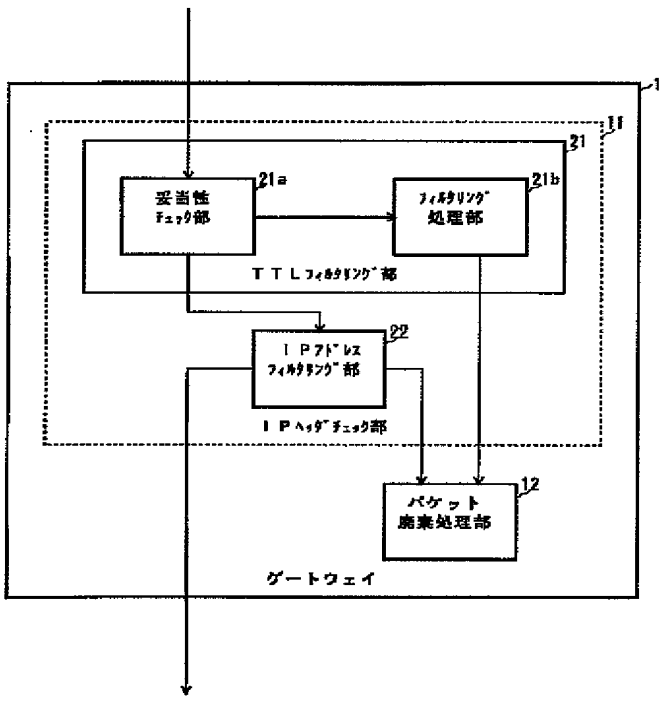
(21)出願番号　特願平9－67929

(22)出願日　平成９年(1997)３月21日

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号
(72)発明者　松岡　芳恵
東京都港区芝浦三丁目18番21号　日本電気エンジニアリング株式会社内
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　不正アクセス防止方法およびシステム

(57)【要約】
【課題】　パケットのデータ形式にエリアの追加を行うことなく、パケットの既存エリアを利用した不正パケットのフィルタリングによる排除を可能とする。
【解決手段】　ゲートウェイ１のＩＰヘッダチェック部１１は、ＩＰヘッダに含まれるＴＴＬ（Time To Live：ネットワーク内存続時間）情報およびＩＰアドレス情報に基づいて、不正でない通信パケットのみを通過させる。ＩＰヘッダチェック部１１のＴＴＬフィルタリング部２１は、ＩＰヘッダ中に妥当性のあるＴＴＬ情報を有する通信パケットのみを通過させる。妥当性チェック部２１ａは、パケット通過時のＴＴＬの値が、予めグループ内で取り決めた初期値から（初期値－最大通過ゲートウェイ数）までの範囲内であることを条件として妥当性をチェックする。フィルタリング処理部２１ｂはＴＴＬ情報が所定の条件を満足していない通信パケットをパケット廃棄処理部１２に与える。



【特許請求の範囲】

【請求項１】　複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、

送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、

前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにした、ことを特徴とする不正アクセス防止方法。

【請求項２】　前記ネットワーク内存続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内存続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断することを特徴とする請求項１に記載の不正アクセス防止方法。

【請求項３】　ＩＰ（インターネットプロトコル）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項１または２に記載の不正アクセス防止方法。

【請求項４】　ＭＡＣ（メディアアクセス制御）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項１乃至３のうちのいずれか１項に記載の不正アクセス防止方法。

【請求項５】　前記不正パケットは、前記結合装置が廃棄することを特徴とする請求項１乃至４のうちのいずれか１項に記載の不正アクセス防止方法。

【請求項６】　複数の支線ネットワークが結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークシステムにおいて、

前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内存続時間情報設定手段を有する端末装置と、

前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段と、を具備することを特徴とする不正アクセス防止システム。

【請求項７】　前記ネットワーク内存続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内存続時間設定手段は、前記機密情報としてのネットワーク内存続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含むことを特徴とする請求項６に記載の不正アクセス防止システム。

【請求項８】　前記ネットワーク結合手段は、ＩＰ（インターネットプロトコル）アドレスに基づくフィルタリングを行うＩＰアドレスフィルタリング手段をさらに含むことを特徴とする請求項６または７に記載の不正アクセス防止システム。

【請求項９】　前記ネットワーク結合手段は、ＭＡＣ（メディアアクセス制御）アドレスに基づくフィルタリングを行うＭＡＣアドレスフィルタリング手段をさらに含むことを特徴とする請求項６乃至８のうちのいずれか１項に記載の不正アクセス防止システム。

【請求項１０】　前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含むことを特徴とする請求項６乃至９のうちのいずれか１項に記載の不正アクセス防止システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信ネットワークシステムを構築するルータおよびゲートウェイ等における不正アクセスの防止に係り、特に、通信プロトコルとしてＴＣＰ／ＩＰ（Transmission Control Protocol / Internet Protocol：転送制御プロトコル／インターネットプロトコル）を使用している通信ネットワークシステムに好適な不正アクセス防止システムに関する。

【０００２】

【従来の技術】通信ネットワークシステム、例えばＬＡＮ（Local Area Network：ローカルエリアネットワーク）システムは、ルータおよびゲートウェイの少なくともいずれかを介して複数の支線ＬＡＮが接続されて構築されている。このような通信ネットワークシステムにおいて、通信プロトコルとしてＴＣＰ／ＩＰを使用していることも多い。

【０００３】ところで、物理的に接続されているネットワーク上で、必要に応じて論理的にグループ分けを行っている場合がある。このような場合、論理的なグループ内での通信が主体となって、他のグループとの間の通信を、必要としなかったり、排除したりしたいことがあ

る。

【０００４】このような場合には、支線ＬＡＮを接続するルータおよびゲートウェイ等において、パケットのＭＡＣ（Media Access Control：メディアアクセス制御）アドレスまたはＩＰ（Internet Protocol：インターネットプロトコル）アドレスを識別し、他のグループのパケットを通過させないようにして、同報パケット、異常パケット、あるいは不正に他のグループの端末にアクセスしようとするパケット等の不正アクセスパケットの流入および流出を防止することが行われている。

【０００５】このように、パケットのＭＡＣアドレスまたはＩＰアドレスを識別して他のグループのパケットは通過させないようにする機能は、ＭＡＣアドレスによりフィルタリングを行うＭＡＣアドレスフィルタリング機能またはＩＰアドレスによりフィルタリングを行うＩＰアドレスフィルタリング機能と称される。

【０００６】すなわち、ＭＡＣアドレスまたはＩＰアドレスによるフィルタリングは、次のようにして行われる。予め通過を許容するＭＡＣアドレスまたはＩＰアドレスを、ルータあるいはゲートウェイに登録しておく。ルータあるいはゲートウェイは、受信したパケットのＭＡＣアドレスまたはＩＰアドレスと登録されているＭＡＣアドレスまたはＩＰアドレスとを照合して、正しいＭＡＣアドレスまたはＩＰアドレスのパケットのみを通過させる。このようにして、不正アクセスパケットの通過がルータあるいはゲートウェイにより阻止される。

【０００７】ＭＡＣアドレスは、多くの場合端末装置（以下、単に「端末」と称する）に物理的に設定されており、安易に変更することができないことが多い。ところが、ＭＡＣ層アドレスには、全ネットワークに同報パケットを通過させるための同報アドレスが存在するため、同報パケットとの混同が生じる。これを防止するために、ＭＡＣ層よりも上位層であるネットワーク層のＩＰアドレスでフィルタリングするＩＰアドレスフィルタリングが用いられる。

【０００８】しかしながら、ＩＰアドレスは、ＴＣＰ／ＩＰプロトコルに必要なものであり、装置に論理的に設定しているため、比較的容易に変更することが可能である。そのため、グループ外の端末が、当該グループ内の端末のＩＰアドレスを不正に設定してグループ内のＬＡＮシステムに入り込もうとした場合には、ＩＰアドレスのフィルタリングでは、不正アクセスパケットを確実に検出することができない。

【０００９】これに対して、特開平７－１７０２７９号公報には、ＩＰアドレスフィルタリングを用いることなく、不正アクセスパケットを排除する技術が開示されている。

【００１０】すなわち、特開平７－１７０２７９号公報に示されたシステムは、ＭＡＣアドレスによるフィルタリングを行う複数の支線ＬＡＮを収容する従来のブリッジ回路に対して、支線ＬＡＮのグループ番号を登録する機能、パケット送信時に該グループ番号をパケットに付加する機能、およびパケットに付加されたグループ番号と登録されたグループ番号とをパケット受信時に照合する機能を付加したブリッジ回路を用いる。

【００１１】このブリッジ回路に収容したＬＡＮそれぞれにグループ番号を設定し、同一グループ内のＬＡＮ間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるＭＡＣアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【００１２】すなわち、複数の端末が接続される複数の支線ＬＡＮを複数のブリッジ回路を介して基幹バスに接続するシステムにおいて、複数のブリッジ回路に個々に収容された複数の支線ＬＡＮを独立した複数のグループにグループ化し、各ブリッジ回路にはそれぞれ収容する支線ＬＡＮのグループ番号を予め登録しておく。端末から同一グループ内の他の支線ＬＡＮへ送信するパケットには、ブリッジ回路は、該端末が属する支線ＬＡＮのグループ番号を付加して基幹バスに送信する。基幹バスを介してパケットを受信したときには、ブリッジ回路は、受信したパケットに付加されているグループ番号を識別し、登録されている番号と照合して、両者が一致したときにのみ、この受信したパケットに対してＭＡＣアドレスフィルタリング機能を動作させブリッジ回路が収容している支線ＬＡＮに送信する。

【００１３】このようにすることにより、ＬＡＮのＭＡＣ層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを、グループ番号の相違により阻止することができる。

【００１４】

【発明が解決しようとする課題】上述したように、特開平７－１７０２７９号公報に示されたシステムは、ブリッジ回路に収容した複数のＬＡＮにそれぞれグループ番号を設定し、同一グループ内のＬＡＮ間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるＭＡＣアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【００１５】この特開平７－１７０２７９号公報のシステムによれば、グループ番号の相違をチェックすることにより、ＬＡＮのＭＡＣ層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを阻止することができる。

【００１６】しかしながら、特開平７－１７０２７９号公報に示された、ブリッジ回路にグループ番号を登録し、送信パケットにこのグループ番号を付加して、パケットを受信したときに受信パケットのグループ番号と登録したグループ番号の照合を行うフィルタリングを可能とするためには、パケットのデータ形式にグループ番号エリアを追加する必要がある。

【００１７】ところが、ＬＡＮのパケットには、物理層のヘッダ部およびトランスポート層のヘッダ部等が含まれており、パケットのデータ形式が細かく規定されていることが多い。したがって、パケットのデータ形式が規定されているＬＡＮシステムにおいては、多くの場合、在来のパケットにグループ番号を格納するためのエリアを追加して確保することができず、特開平７－１７０２７９号公報に記載された技術を実施することができない。

【００１８】この発明は、上述した事情に鑑みてなされたもので、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することを目的とする。

【００１９】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る不正アクセス防止方法は、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにする。

【００２０】前記ネットワーク内存続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内存続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断するようにしてもよい。

【００２１】前記不正アクセス防止方法は、さらに、ＩＰアドレスに基づくフィルタリングをさらに併用するようにしてもよい。

【００２２】前記不正アクセス防止方法は、さらに、ＭＡＣアドレスに基づくフィルタリングをさらに併用するようにしてもよい。

【００２３】前記不正アクセス防止方法は、前記不正パケットを、前記結合装置が廃棄するようにしてもよい。

【００２４】この発明の第２の観点に係る不正アクセス防止システムは、複数の支線ネットワークが結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークシステムにおいて、前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内存続時間情報設定手段を有する端末装置と、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段と、を具備する。

【００２５】前記ネットワーク内存続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内存続時間設定手段は、前記機密情報としてのネットワーク内存続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含んでいてもよい。

【００２６】前記ネットワーク結合手段は、ＩＰアドレスに基づくフィルタリングを行うＩＰアドレスフィルタリング手段をさらに含んでいてもよい。

【００２７】前記ネットワーク結合手段は、ＭＡＣアドレスに基づくフィルタリングを行うＭＡＣアドレスフィルタリング手段をさらに含んでいてもよい。

【００２８】前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含んでいてもよい。

【００２９】この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリン

グを行う。したがって、パケットの既存エリアであるネットワーク内存続時間情報を利用して不正パケットのフィルタリングを行うことができ、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除が可能となる。

【００３０】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

【００３１】この発明の実施の形態に係る不正アクセス防止システムは、ＴＣＰ／ＩＰプロトコルを用いた通信ネットワークシステムに適用している。この実施の形態では、ＴＣＰ／ＩＰプロトコルのＩＰヘッダ内の既存のエリアであるＴＴＬを利用することにより不正パケットのフィルタリングを行うことにより、通信パケットの在来のデータ形式のままで不正アクセスを効果的に防止する。

【００３２】ＴＣＰ／ＩＰプロトコルによる通信パケットのＩＰヘッダには、ＴＴＬ（Timeto Live：ネットワーク内存続時間）情報を格納するためのＴＴＬエリアが設けられている。ＴＴＬ情報とは、通信パケットが、あとどれだけの時間ネットワーク内に存続できるか、すなわち存続残時間を秒単位で示したものである。この存続算時間は、秒単位を基本としているが、処理時間が１秒に満たない場合および処理時間が計測できない場合があり、一般に、例えばルータまたはゲートウェイのような結合装置を通過する度に、その都度“１”マイナスされ、このＴＴＬの値が“０”である通信パケットを検出したときに、その通信パケットは、存続時間が満了したものとして廃棄される。このようなＴＴＬ情報は、永遠に配達されずに、ネットワーク中を浮遊するパケットが発生することを防止するために設けられている。ＴＣＰ／ＩＰプロトコルにおいては、ＴＴＬの最大値は“２５５（秒）”である。一般には、送信端末から受信端末までのルータおよびゲートウェイ等の結合装置の数は、不達パケットの発生を防止するために多めに見積もられる。しかも、このＴＴＬの値は、仮に最大値を設定しても送信から２５５秒たった時点で通信パケットが廃棄されるため、通常の場合、かなり大きめに設定される。

【００３３】この発明では、論理的なグループ内で、ＴＴＬの初期値を機密情報として予め取り決めておき、グループ内の送信端末から受信端末までにパケットが通過すると予想されるルータおよびゲートウェイ等の結合装置の最大数を設定しておく。この結合装置の最大数よりも、ＴＴＬの初期値を大きく設定しておく。パケットのフィルタリングにあたっては、パケット通過時のＴＴＬの値がＴＴＬの初期値から（初期値－最大通過結合装置数）までの範囲であれば正常パケット、該範囲外であれば不正パケットと判断する。

【００３４】このような仕組みにより、グループ内の端末のＩＰアドレスを使用して不正にグループ内の端末にアクセスしようとするグループ外の不正な端末からの不正パケットを排除することができる。

【００３５】図１～図３を参照して、上述した原理に基づくこの発明による不正アクセス防止システムを組み込んだネットワークシステムの実施の形態を説明する。

【００３６】図１は、この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示している。

【００３７】図１に示すゲートウェイ１は、ＩＰヘッダチェック部１１およびパケット廃棄処理部１２を具備している。

【００３８】ＩＰヘッダチェック部１１は、ＩＰヘッダの情報をチェックし、ＩＰヘッダに含まれるＴＴＬ（Time to Live：ネットワーク内存続時間）情報およびＩＰアドレス情報に基づいて、当該論理グループの内部から外部へ、および外部から内部への通過パケットをチェックして、不正でない通信パケットのみを通過させ、不正パケットの通過を阻止する。パケット廃棄処理部１２は、ＩＰヘッダチェック部１１により、通過が阻止された不正パケットを廃棄処理する。

【００３９】ＩＰヘッダチェック部１１は、ＴＴＬフィルタリング部２１およびＩＰアドレスフィルタリング部２２を有する。

【００４０】ＴＴＬフィルタリング部２１は、妥当性チェック部２１ａおよびフィルタリング処理部２１ｂを有し、ＩＰヘッダ中のＴＴＬ情報の妥当性をチェックして、ＴＴＬ情報として妥当性のあるＴＴＬ情報を有する通信パケットのみを通過させ、妥当性のないＴＴＬ情報を有する通信パケットの通過を阻止する。

【００４１】妥当性チェック部２１ａは、通信パケットの通過時にＩＰヘッダにおけるＴＴＬ情報が所定の条件を満足しているか否かに基づいて、ＴＴＬ情報の妥当性をチェックする。フィルタリング処理部２１ｂは、論理グループの内外間での通過パケットに対し、妥当性チェック部２１ａのチェック結果に基づいて、ＴＴＬ情報が所定の条件を満足している通信パケットのみを通過させ、該所定の条件を満足していない通信パケットをパケット廃棄処理部１２に与える。

【００４２】上述したようにゲートウェイ１におけるＴＴＬ情報を用いたフィルタリングでは、各論理グループにおいて、予めグループ内でのＴＴＬの初期値を機密データとして取り決め、且つグループ内の送信端末から受信端末までにパケットが通過する結合装置、例えばゲートウェイおよびルータ等、の最大数を設定しておく。そして、これらＴＴＬの初期値と最大通過結合装置数をゲートウェイ１の妥当性チェック部２１ａに予め登録しておくことにより、妥当性チェック部２１ａは、パケット通過時のＴＴＬの値がＴＴＬの初期値から（初期値－最大通過ゲートウェイ数）までの範囲内であるか否かを条件として妥当性をチェックする。ＴＴＬの値が該範囲内

であれば正常パケットすなわち妥当性ありと判定し、当該範囲外であれば不正パケットすなわち妥当性なしと判定する。

【００４３】ＩＰアドレスフィルタリング部２２は、ＩＰヘッダにおけるＩＰアドレス情報に基づいて、当該論理グループの外部から該論理グループの内部のアドレスへの通信パケットおよび当該論理グループの内部から該論理グループの外部のアドレスへの通信パケットを通過させ、それ以外のＩＰアドレス情報を有する通信パケットの通過を阻止してパケット廃棄処理部１２に与える。

【００４４】図１に示したゲートウェイ１を用いて構成したネットワークシステムを図２に示す。図２においては、在来のフィルタリング機能を有するゲートウェイと図１のこの発明によるフィルタリング機能を有するゲートウェイとを用いて不正アクセス防止システムを構成している。

【００４５】図２に示すネットワークシステムは、第１のゲートウェイ１、第２のゲートウェイ２、第１の端末３、第２の端末４、第３の端末５、第１の支線ＬＡＮ６、第２の支線ＬＡＮ７および第３の支線ＬＡＮ８を備えている。第１の端末３および第２の端末４は、第１の支線ＬＡＮ６に結合されており、第３の端末５は第３の支線ＬＡＮ８に結合されている。第１の支線ＬＡＮ６と第２の支線ＬＡＮ７とは第２のゲートウェイ２により結合されており、第２の支線ＬＡＮ７と第３の支線ＬＡＮ８とは第２のゲートウェイ１により結合されている。

【００４６】第１および第２のゲートウェイ１および２は、それぞれ第２の支線ＬＡＮ７と第３の支線ＬＡＮ８との間、および第１の支線ＬＡＮ６と第２の支線ＬＡＮ７との間で通信パケット等のデータを転送する。

【００４７】第１のゲートウェイ１は、図１に示したこの発明に基づく通信パケットのフィルタリング機能を有するゲートウェイである。すなわち、第１のゲートウェイ１は、この発明によるＴＴＬ情報を用いた通信パケットのフィルタリング機能と、在来のＩＰアドレスを用いた通信パケットのフィルタリング機能とを有している。

【００４８】第２のゲートウェイは、在来のゲートウェイであり、ＩＰアドレスを用いた通信パケットのフィルタリング機能のみを有している。

【００４９】第２の端末４および第３の端末５が同一グループを構成し、第１の端末３はグループ外の端末であるとする。

【００５０】この場合、例えば、端末４と端末５とで構成されるグループ内では、機密データとしてＴＴＬの初期値を“５”と設定しているものとする。また、最大通過結合装置数、すなわち最大通過ゲートウェイ数は、ゲートウェイ１および２が存在するため“２”である。これらの値は、ゲートウェイ１の妥当性チェック部２１ａに予め設定される。

【００５１】グループ外の端末３は、端末４と端末５とのグループ間で取り決めたＴＴＬの初期値がわからないため、端末３では、ＴＴＬの初期値を“３２”と設定したものとする。端末４が端末５に通信パケットを送信したときの動作、および端末４が支線ＬＡＮ６に接続していない状態で端末３が端末４を装って、端末４のＩＰアドレスに設定して、端末５に不正にアクセスしようとした場合の動作について、図３に示すフローチャートを参照して説明する。図３に示すフローチャートは、図１のゲートウェイ１のＩＰヘッダチェック部１１におけるＩＰヘッダのチェック処理の流れを示している。

【００５２】ゲートウェイ２にはＩＰアドレスのフィルタリングのみを行うために端末４と端末５のＩＰアドレスを登録する。ゲートウェイ１には、ＩＰアドレスのフィルタリングのために端末４と端末５のＩＰアドレスを登録し、且つＴＴＬによるフィルタリングのために、端末４と端末５との間で取り決めたＴＴＬの初期値α“５”と最大通過ゲートウェイ数“２”とを内部の妥当性チェック部２１ａに記憶させる。

【００５３】まず、端末４が同一グループ内の端末５に通信パケットを送信する場合の動作について説明する。

【００５４】端末４は、自分のＩＰアドレス、つまり発信元ＩＰアドレス、に端末４のＩＰアドレスを設定し、相手のＩＰアドレス、つまり宛先（送信先）ＩＰアドレスに相手先端末５のＩＰアドレスを設定するとともに、ＴＴＬには当該グループ間で取り決めた初期値α“５”をセットして、通信パケットを支線ＬＡＮ６に送信する。

【００５５】送信されたパケットは、ゲートウェイ２で受信される。ゲートウェイ２は、ＩＰヘッダをチェックする。ゲートウェイ２は、発信元ＩＰアドレスが登録されている端末４のアドレスであり、宛先ＩＰアドレスが登録されている端末５のアドレスであるため、正常パケットとみなす。正常パケットとみなすと、ゲートウェイ２は、元のＴＴＬ値である“５”から“１”をマイナスした“４”を新たなＴＴＬ値としてＴＴＬにセットして、通信パケットを支線ＬＡＮ７に送信する。

【００５６】支線ＬＡＮ７に送信されたパケットは、さらにゲートウェイ１で受信される。ゲートウェイ１は、ＩＰヘッダチェック部１１において、図３に示すフローチャートに従ってＩＰヘッダのチェックを行う。

【００５７】ＩＰヘッダのチェックが開始されると、ＩＰのバージョンのチェックを行い（ステップＳ１１）、バージョンが異常である場合は、パケット廃棄処理部１２でパケットを廃棄する（ステップＳ１７）。ステップＳ１１で、バージョンが正常であった場合は、ＩＰヘッダのその他の情報のチェックを行い（ステップＳ１２）、該その他の情報の異常を検知した場合にもステップＳ１７に移行してパケットを廃棄する。

【００５８】ステップＳ１２で正常であった場合には、ＴＴＬの値が“０”であるか否かのチェックを行う（ス

テップＳ１３）。ステップＳ１３において、ＴＴＬの値が“０”である場合には、ＴＴＬすなわちネットワーク内存続時間が満了しているので、ステップＳ１７でパケットを廃棄する。この場合には、ＴＴＬの値は、“４”であるので、ステップＳ１３では正常と判定され、ＴＴＬフィルタリング部２１の妥当性チェック部２１ａでＴＴＬの値の妥当性のチェックを行う（ステップＳ１４）。

【００５９】妥当性のチェックは、ＴＴＬの値が初期値α以下で且つ（初期値－最大ゲート数）βを超えているか否かにより行う。ＴＴＬの値がこの範囲内であれば妥当であるとみなす。

【００６０】この場合、初期値αは“５”、（初期値－最大ゲート数）βは“３”（＝５－２）であり、受信したパケットのＴＴＬの値は“４”であるため、正常とみなされる。ステップＳ１４で正常とみなされると、ＩＰアドレスフィルタリング部１２によりＩＰアドレスのチェックを行う（ステップＳ１５）。ステップＳ１４で不正とみなされた場合には、ステップＳ１７でパケットを廃棄する。

【００６１】受信した通信パケットの発信元ＩＰアドレスは登録されている端末４のＩＰアドレスであり、宛先ＩＰアドレスは登録されている端末５のアドレスであるため、正常パケットとみなし、通信パケットは、ゲートウェイ１に受信される（ステップＳ１６）。ゲートウェイ１は、受信したパケットのＴＴＬに“４”から“１”をマイナスした“３”をセットして、通信パケットを支線ＬＡＮ８に送信する。送信された通信パケットは相手先端末である端末５で受信される。

【００６２】次に、端末４が支線ＬＡＮ６に接続されていない状態で、当該グループ外の端末３が端末４を装って不正に端末５にパケットを送信しようとした場合の動作を説明する。

【００６３】端末３は、発信元ＩＰアドレスに端末４のＩＰアドレスを設定し、宛先ＩＰアドレスに相手先端末５のＩＰアドレスを設定して、通信パケットを支線ＬＡＮ６に送信する。しかしこの場合、端末３では、相手先端末５が属する論理グループに属していないので、当該グループ内で取り決めたＴＴＬの初期値がわからない。そのため、端末３は、適当な値として“３２”をＴＴＬにセットして通信パケットを送信する。

【００６４】送信された通信パケットはゲートウェイ２に受信される。ゲートウェイ２は、ＩＰアドレスのフィルタリングのためのＩＰヘッダのチェックを行うが、発信元ＩＰアドレスが登録されている端末４のアドレスであり、宛先ＩＰアドレスが登録されている端末５のアドレスであるため、ＩＰアドレスは正常であるとみなす。そこで、ゲートウェイ２は、“３２”から“１”をマイナスした“３１”をＴＴＬにセットして、該通信パケットを支線ＬＡＮ７に送信する。

【００６５】支線ＬＡＮ７に送信されたパケットはゲートウェイ１で受信される。ゲートウェイ１は、ＩＰヘッダチェック部１１において、図３に示すフローチャートに従ってＩＰヘッダのチェックを行う。

【００６６】ＩＰヘッダのチェックが開始されると、ステップＳ１１でＩＰのバージョンのチェックを行い、バージョンが異常である場合は、ステップＳ１７に移行しパケット廃棄処理部１２でパケットを廃棄する。ステップＳ１１で、バージョンが正常であった場合は、ステップＳ１２で、ＩＰヘッダのその他の情報のチェックを行い、異常を検知した場合には、ステップＳ１７でパケットを廃棄する。

【００６７】ステップＳ１２で、ＩＰヘッダのその他の情報が正常であった場合には、ステップＳ１３で、ＴＴＬの値が“０”であるか否かのチェックを行う。ステップＳ１３のチェックにおいて、もしもＴＴＬの値が“０”であればパケットを廃棄するが、この場合は、ＴＴＬの値が“３１”であるため、ステップＳ１３では正常と判定され、ステップＳ１４でＴＴＬの値の妥当性のチェックを行う。

【００６８】ステップＳ１４の妥当性のチェックにおいて、先に述べたように初期値αは“５”であり、（初期値－最大通過ゲートウェイ数）であるβは“３”（＝５－２）であるが、受信した通信パケットのＴＴＬの値は“３１”であるため、異常とみなされ、ステップＳ１７に移行して、該通信パケットは廃棄される。

【００６９】上述したように、ＩＰヘッダ部分におけるＴＴＬを利用したフィルタリング機能により、ＩＰアドレスフィルタリングでは検出することができない不正パケットを検出し、廃棄して、端末の不正アクセス防止機能の信頼性を向上することができる。

【００７０】なお、図１～図３で説明したこの発明の実施の形態においては、ＴＴＬ情報を利用したフィルタリングに、ＩＰアドレスによるフィルタリングを併用するものとしたが、さらにＭＡＣアドレスに基づくフィルタリング処理を行う手段を設けて、ＭＡＣアドレスフィルタリング機能を併用するようにしてもよい。

【００７１】

【発明の効果】以上説明したように、この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行う。したがって、パケッ

トの既存エリアであるネットワーク内存続時間情報を利用して不正パケットのフィルタリングを行うことができる。

【００７２】すなわち、この発明によれば、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することができる。

【図面の簡単な説明】

【図１】この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示すブロック図である。

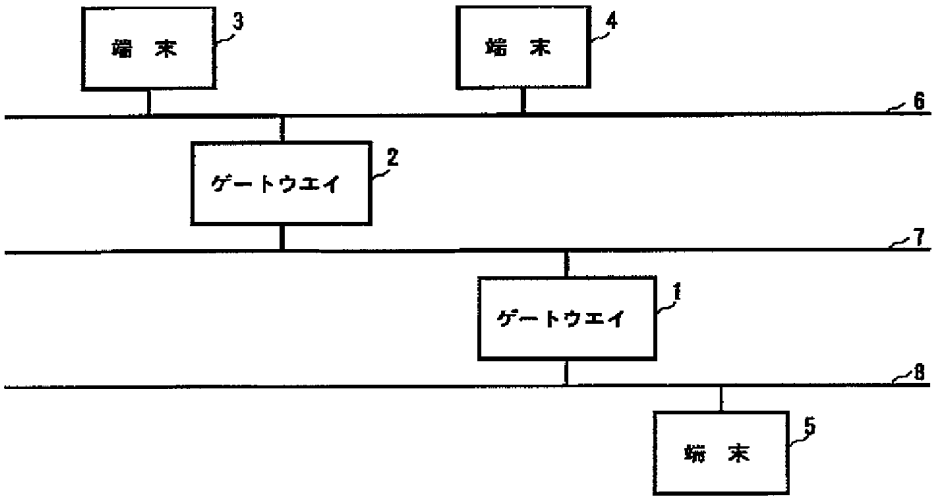
【図２】図１のゲートウェイを用いたネットワークシステムの構成を示すブロック図である。

【図３】図１のシステムの動作を説明するため、ゲートウェイのＩＰヘッダチェック部におけるＩＰヘッダのチェックの流れを示すフローチャートである。

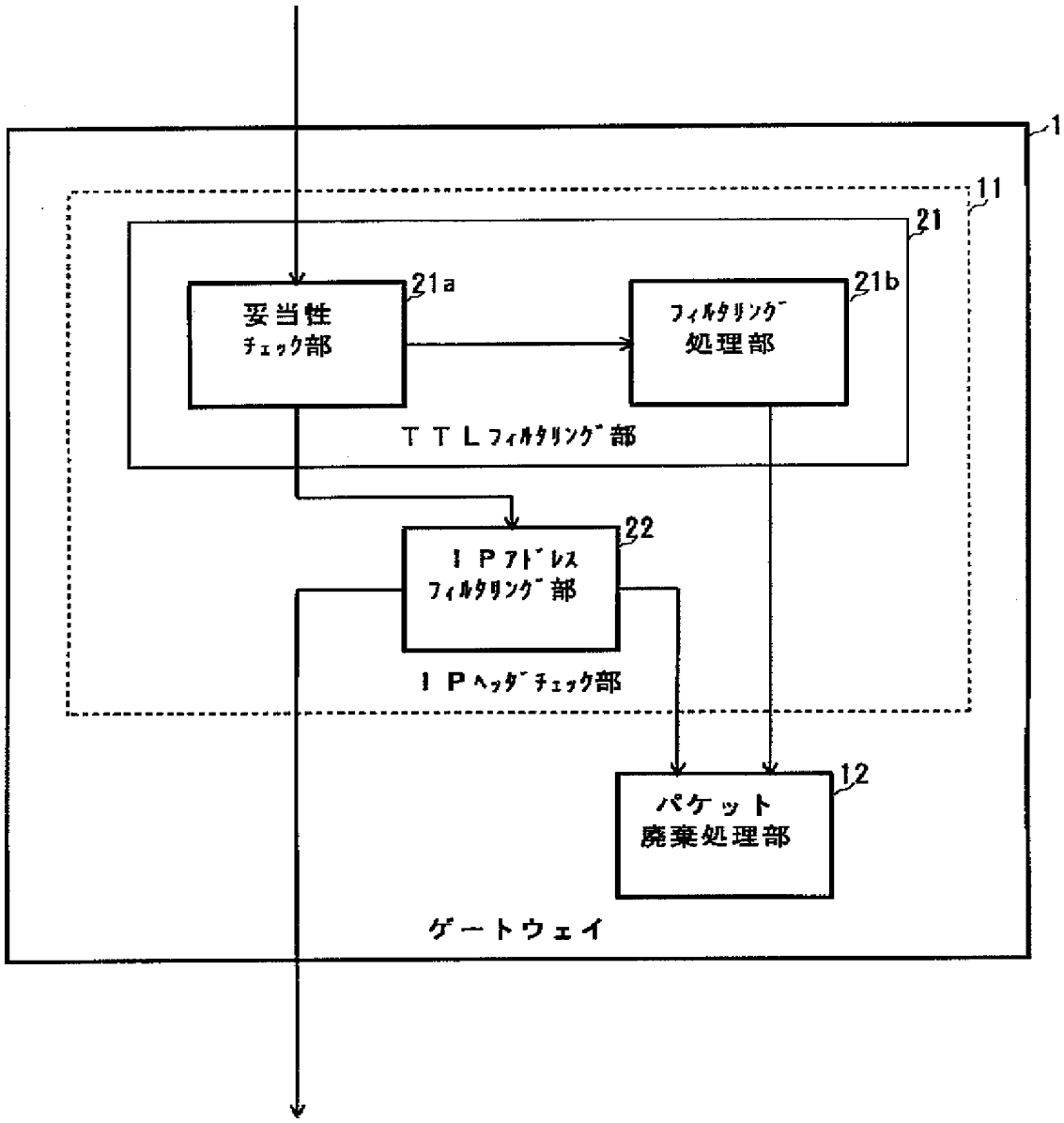
【符号の説明】

１，２　ゲートウェイ
３～５　端末（端末装置）
６～８　支線ＬＡＮ（Local Area Network）
１１　ＩＰ（Internet Protocol）ヘッダチェック部
１２　パケット廃棄処理部
２１　ＴＴＬ（Time to Live）フィルタリング部
２１ａ　妥当性チェック部
２１ｂ　フィルタリング処理部
２２　ＩＰアドレスフィルタリング部

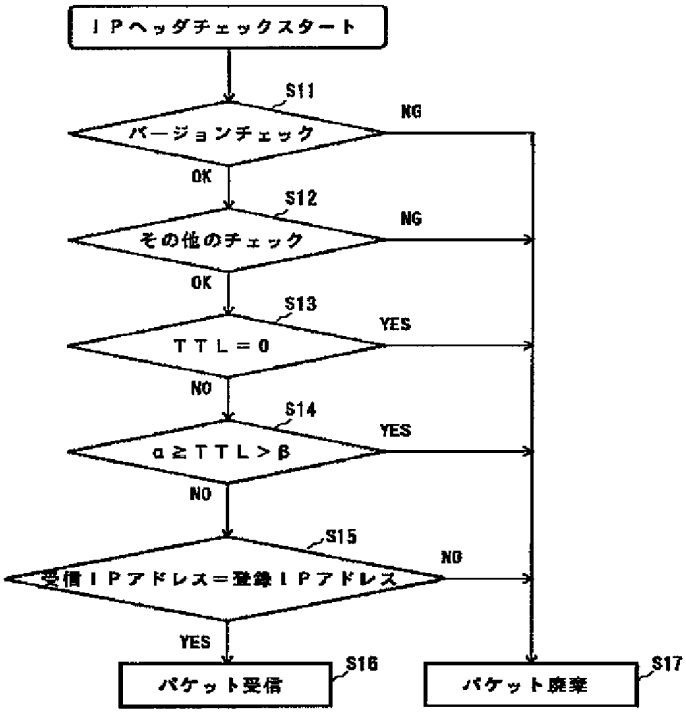
【図２】



【図１】


1
11
21
21a
妥当性
ﾁｪｯｸ部
21b
ﾌｨﾙﾀﾘﾝｸﾞ
処理部
ＴＴＬﾌｨﾙﾀﾘﾝｸﾞ部
22
ＩＰｱﾄﾞﾚｽ
ﾌｨﾙﾀﾘﾝｸﾞ部
ＩＰﾍｯﾀﾞﾁｪｯｸ部
12
パケット
廃棄処理部
ゲートウェイ

【図３】



α：ＴＴＬ初期値
β：ＴＴＬ初期値－最大通過ｹﾞｰﾄｳｪｲ数